RSAC 2025 Conference

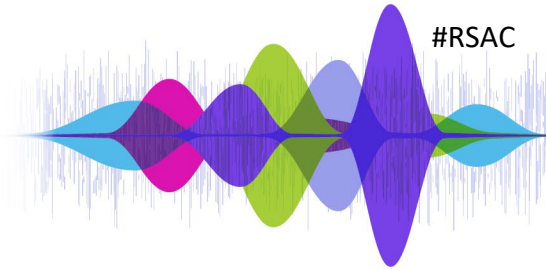
Many Voices.
One Community.

SESSION ID: IDY-M03

From Ideal to Real: Demystifying Passkey Concepts and Implementations

Fei Liu

Senior Emerging Tech Researcher
Okta
https://www.linkedin.com/in/fei-liu-87979812/



Disclaimer

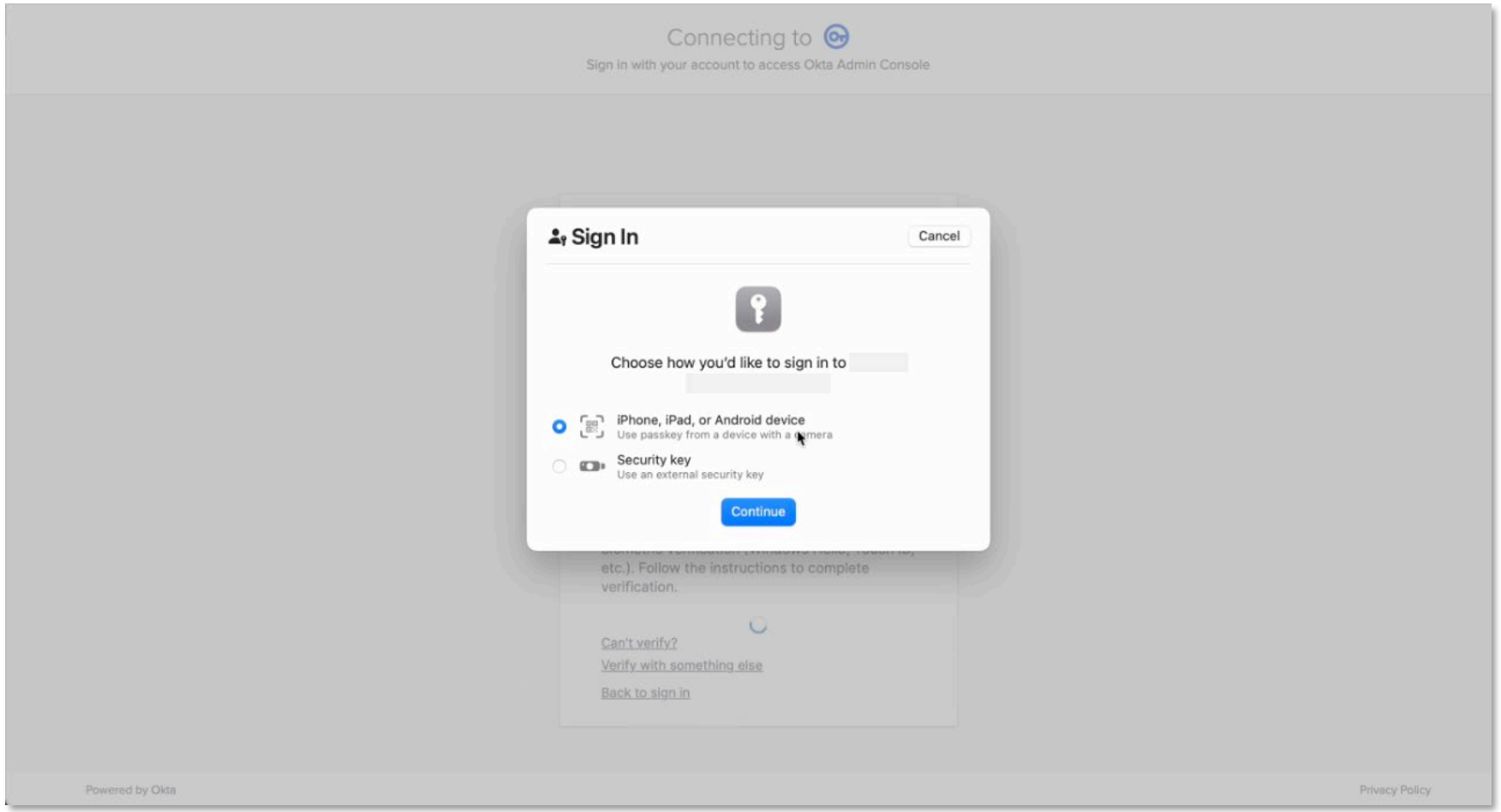
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

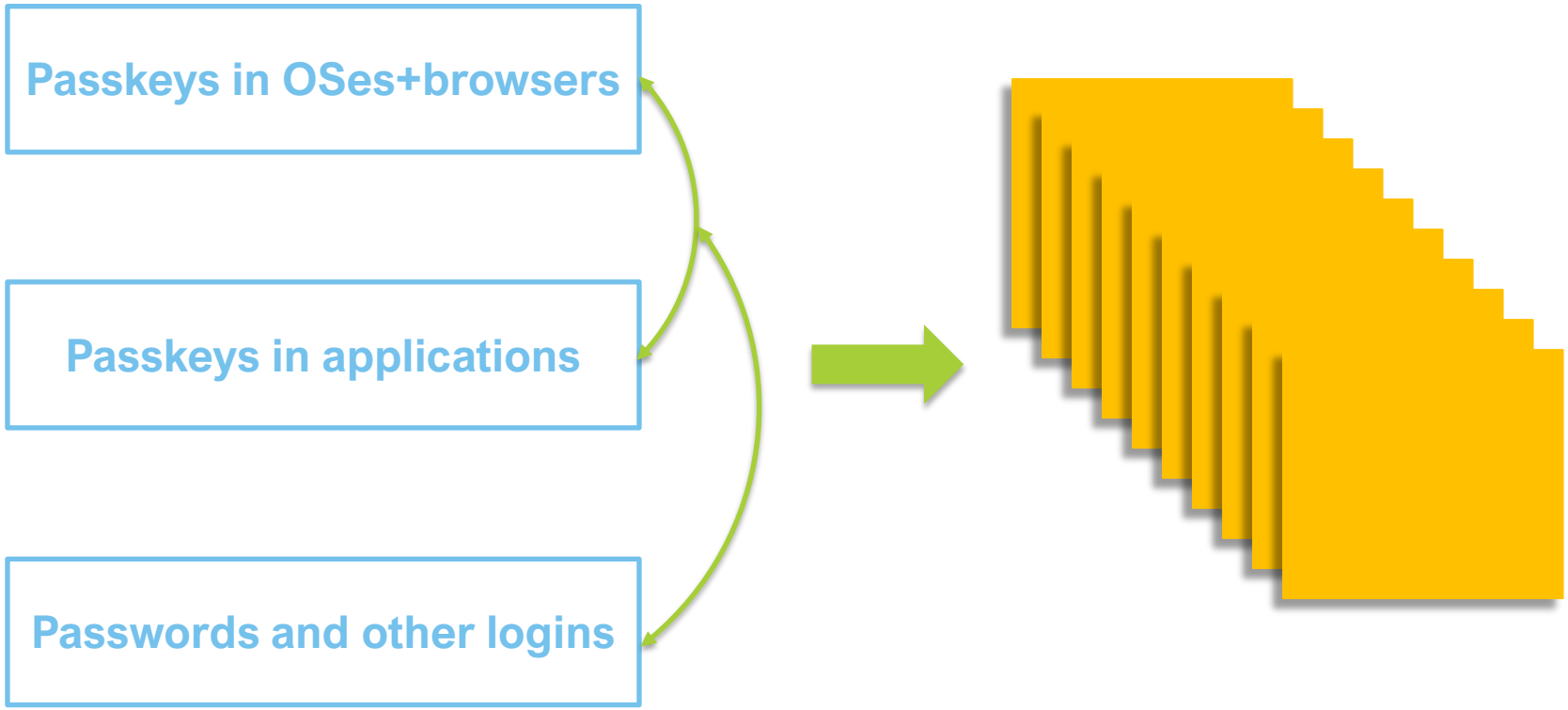
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements.

A passkey sign-in/sign-up pain


Connecting to
Sign in with your account to access Okta Admin Console
Sign In
Cancel
Choose how you'd like to sign in to
iPhone, iPad, or Android device
Use passkey from a device with a camera
Security key
Use an external security key
Continue
etc.). Follow the instructions to complete verification.
Can't verify?
Verify with something else
Back to sign in
Powered by Okta
Privacy Policy

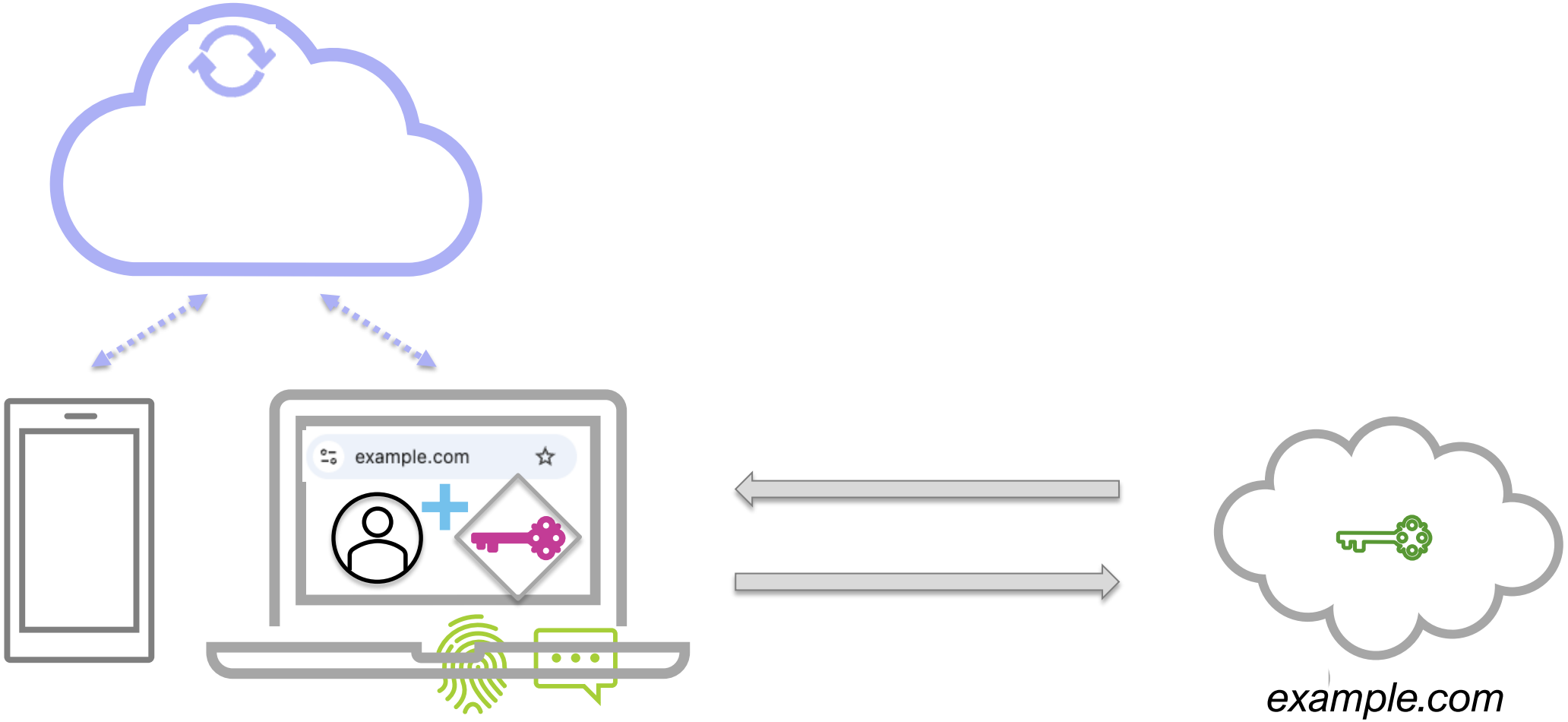
Methodology



RSAC 2025 Conference

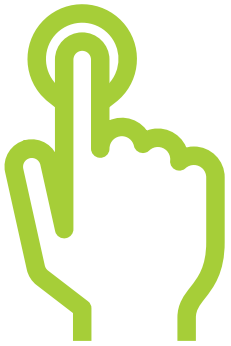
Ideal: Passkey Basics

What are passkeys



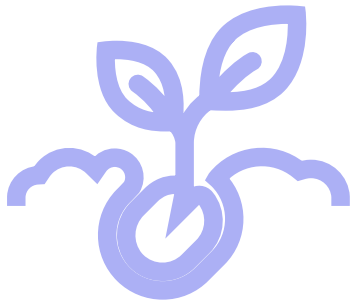
Passkeys have enormous potential benefits

Usability



Security

Adoption

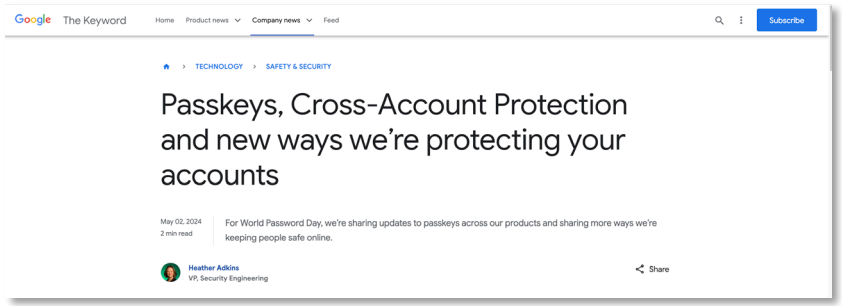


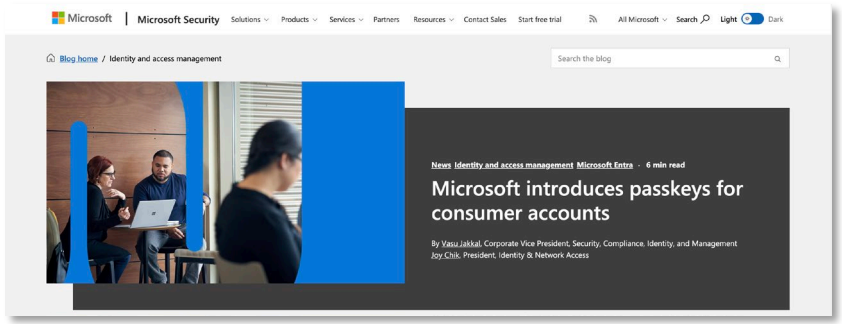
RSAC 2025 Conference

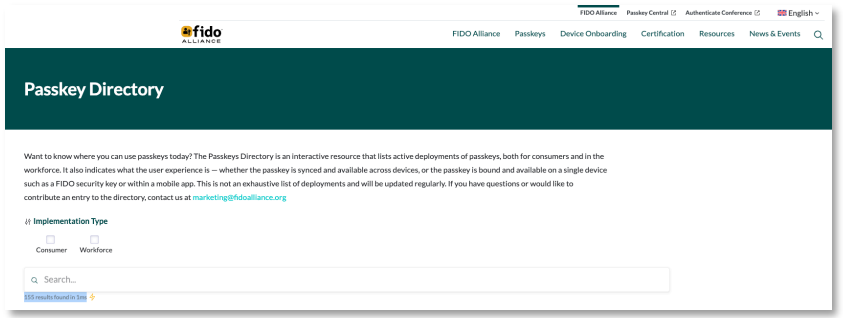
Real: Snapshot of the Current State of Passkeys

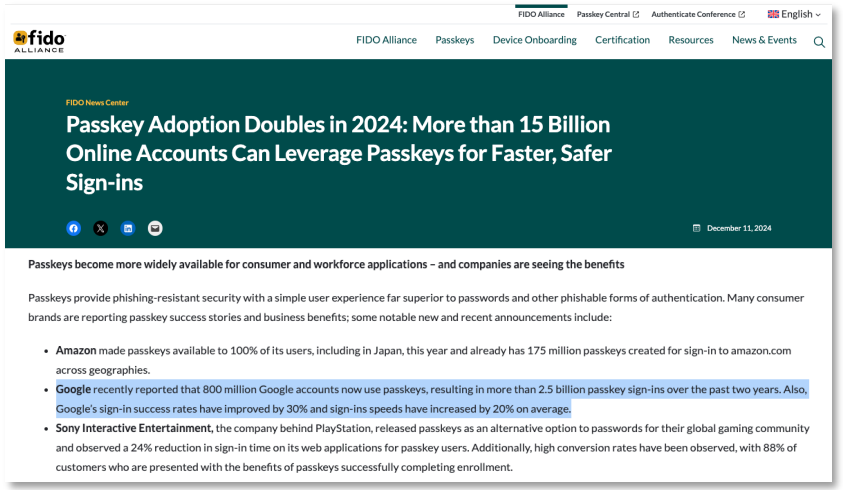
Passkeys have gained popularity.

Passkey news are exciting



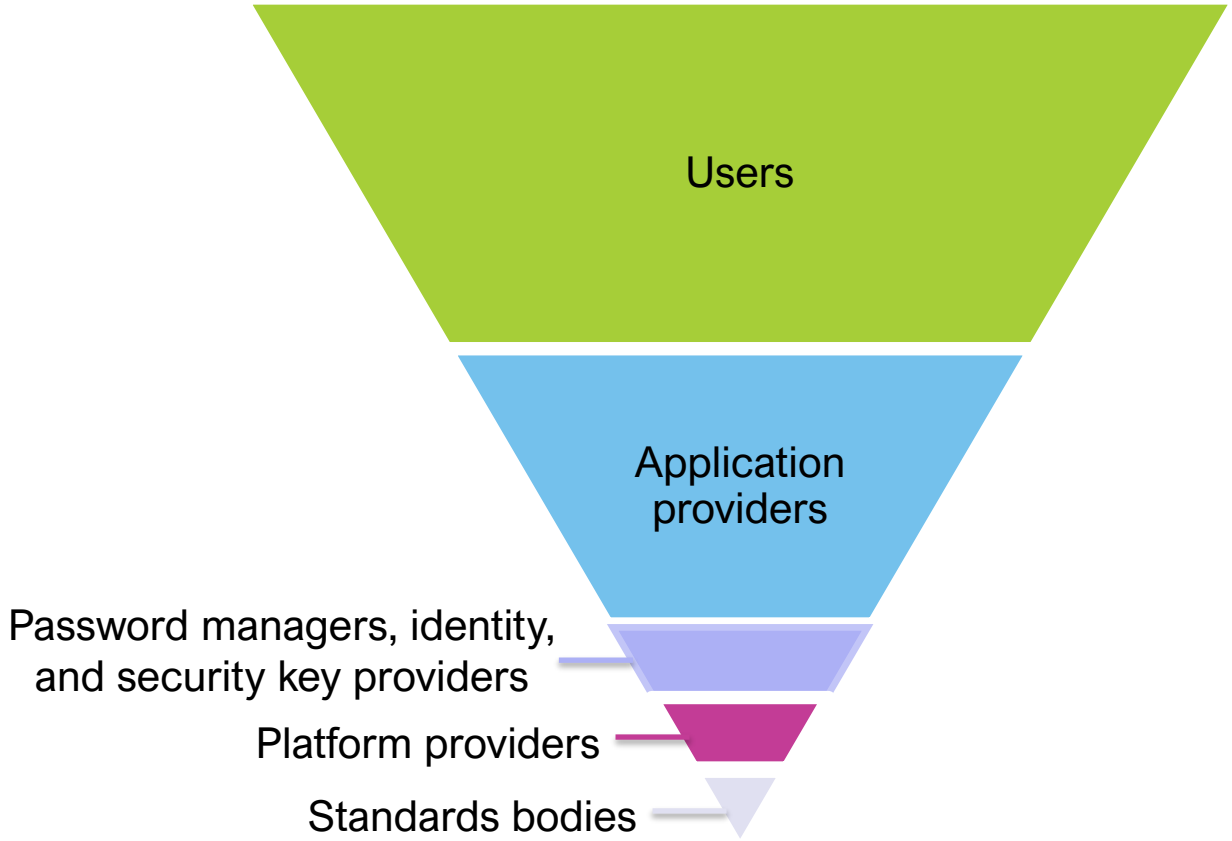



FIDO Alliance
Passkey Central
Authenticate Conference
English
fido ALLIANCE
FIDO Alliance
Passkeys
Device Onboarding
Certification
Resources
News & Events
Passkey Directory
Want to know where you can use passkeys today? The Passkeys Directory is an interactive resource that lists active deployments of passkeys, both for consumers and in the workforce. It also indicates what the user experience is — whether the passkey is synced and available across devices, or the passkey is bound and available on a single device such as a FIDO security key or within a mobile app. This is not an exhaustive list of deployments and will be updated regularly. If you have questions or would like to contribute an entry to the directory, contact us at marketing@fidoalliance.org
Implementation Type
Consumer
Workforce
Search...
155 results found in 3ms

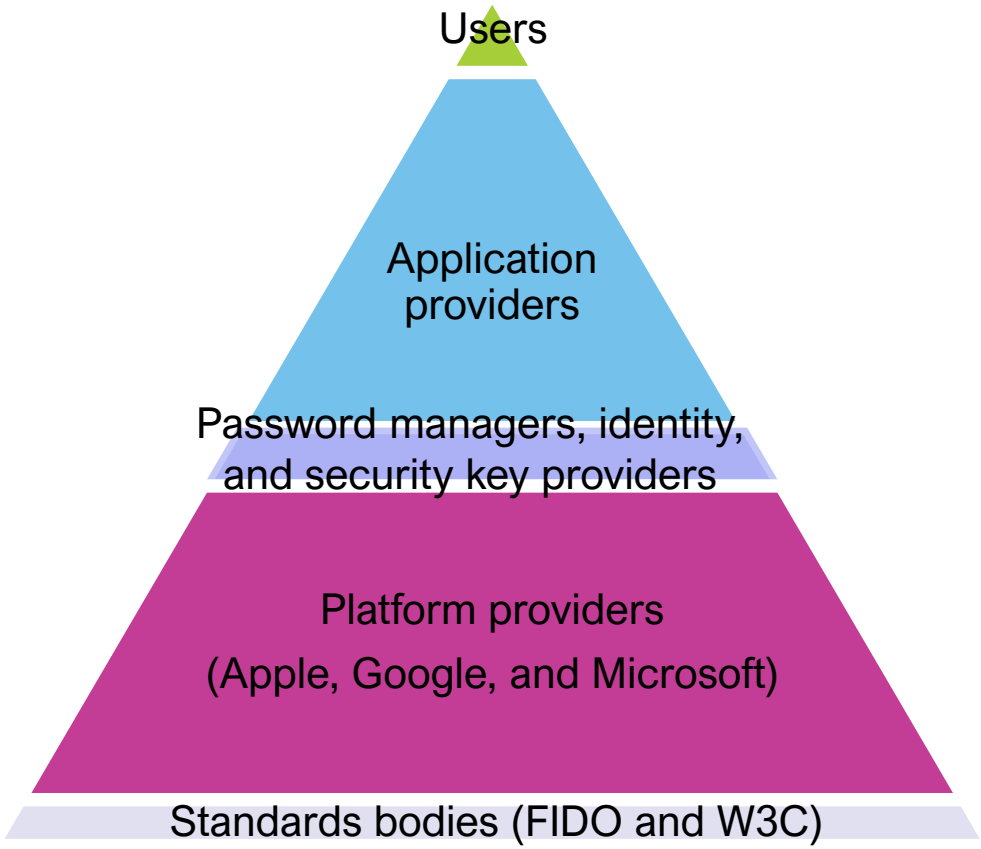

FIDO Alliance
Passkey Central
Authenticate Conference
English
fido ALLIANCE
FIDO Alliance
Passkeys
Device Onboarding
Certification
Resources
News & Events
FIDO News Center
Passkey Adoption Doubles in 2024: More than 15 Billion Online Accounts Can Leverage Passkeys for Faster, Safer Sign-ins
December 11, 2024
Passkeys become more widely available for consumer and workforce applications – and companies are seeing the benefits
Passkeys provide phishing-resistant security with a simple user experience far superior to passwords and other phishable forms of authentication. Many consumer brands are reporting passkey success stories and business benefits; some notable new and recent announcements include:
Amazon made passkeys available to 100% of its users, including in Japan, this year and already has 175 million passkeys created for sign-in to amazon.com across geographies.
Google recently reported that 800 million Google accounts now use passkeys, resulting in more than 2.5 billion passkey sign-ins over the past two years. Also, Google's sign-in success rates have improved by 30% and sign-ins speeds have increased by 20% on average.
Sony Interactive Entertainment, the company behind PlayStation, released passkeys as an alternative option to passwords for their global gaming community and observed a 24% reduction in sign-in time on its web applications for passkey users. Additionally, high conversion rates have been observed, with 88% of customers who are presented with the benefits of passkeys successfully completing enrollment.

Passkey ecosystem is flourishing

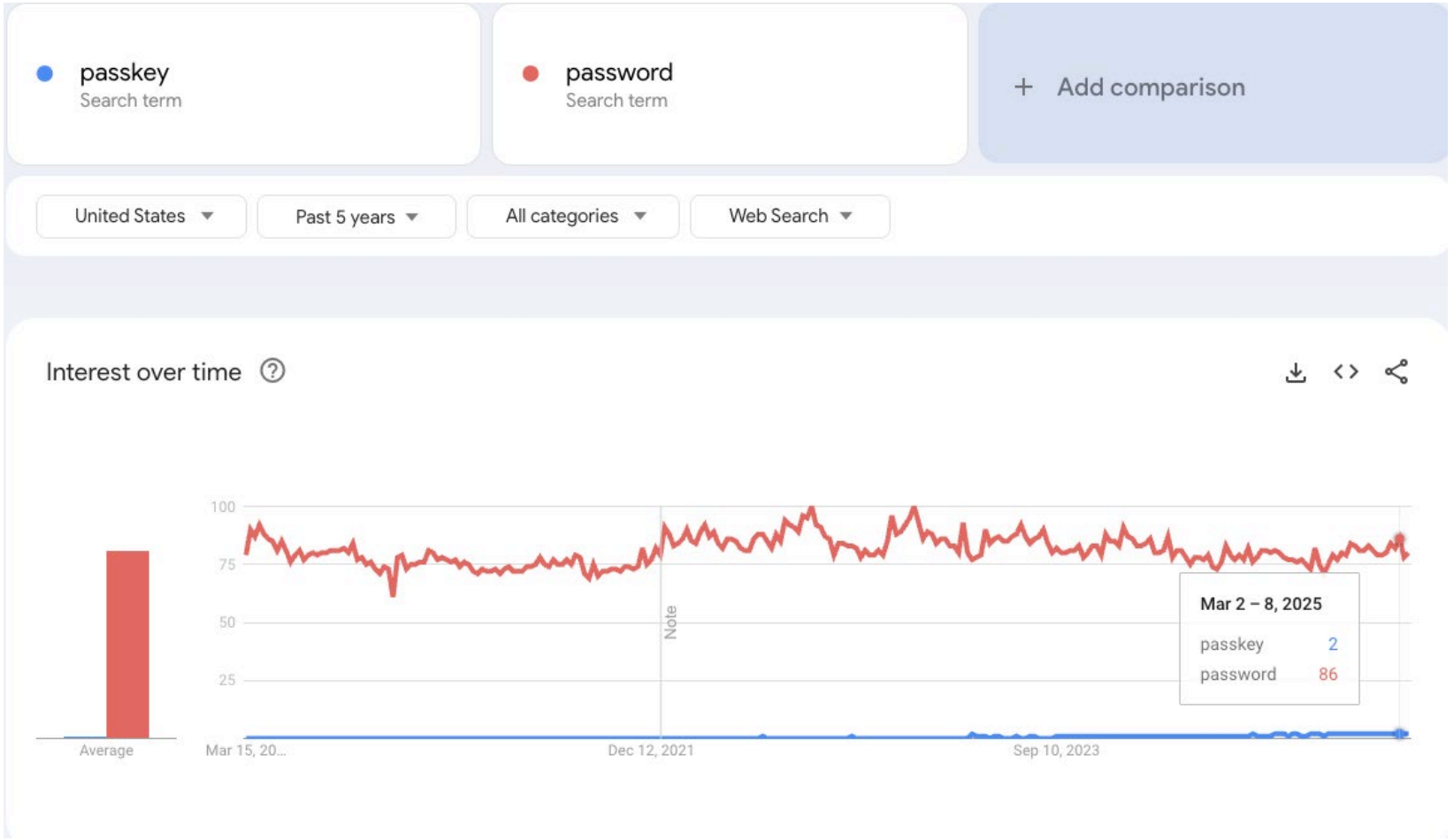
Ecosystem players by count



Ecosystem players by power



But why do passwords still dominate digital life?



Passkeys are always synced credentials.

FIDO2 standards and terminology evolution

2018

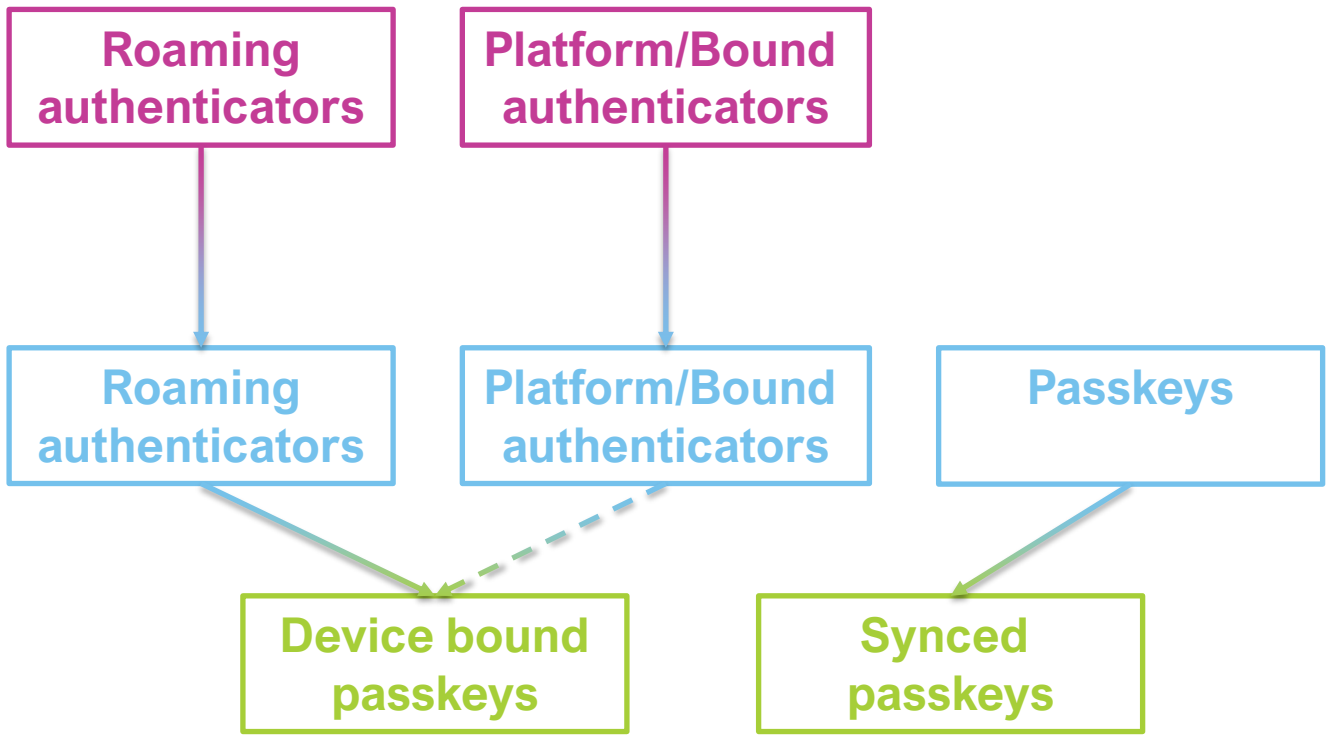
FIDO2 standards were released

2022

Passkeys were introduced

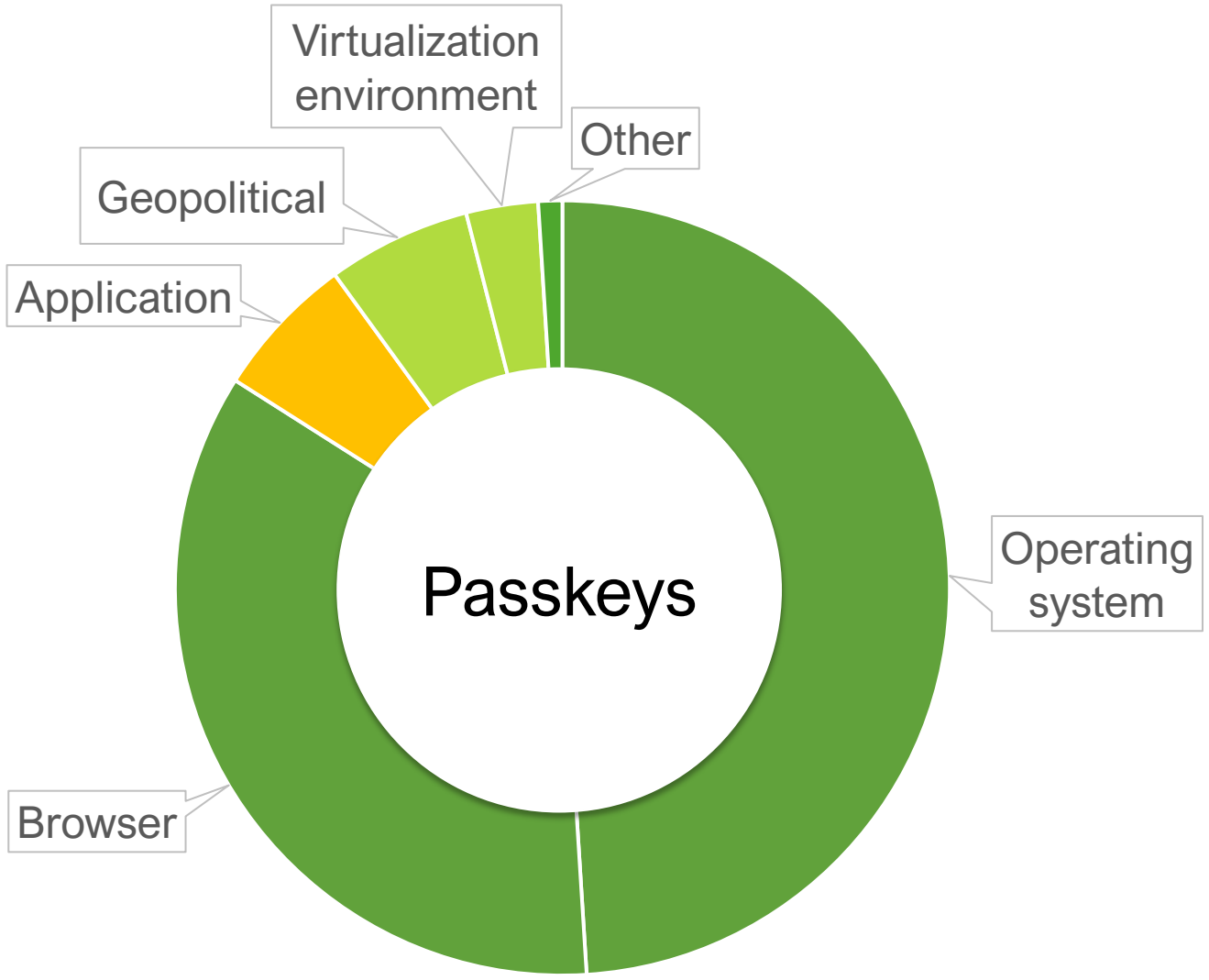
2023

Passkeys = discoverable FIDO credentials



Passkeys are universally available online.

Passkeys depend on their tech stacks

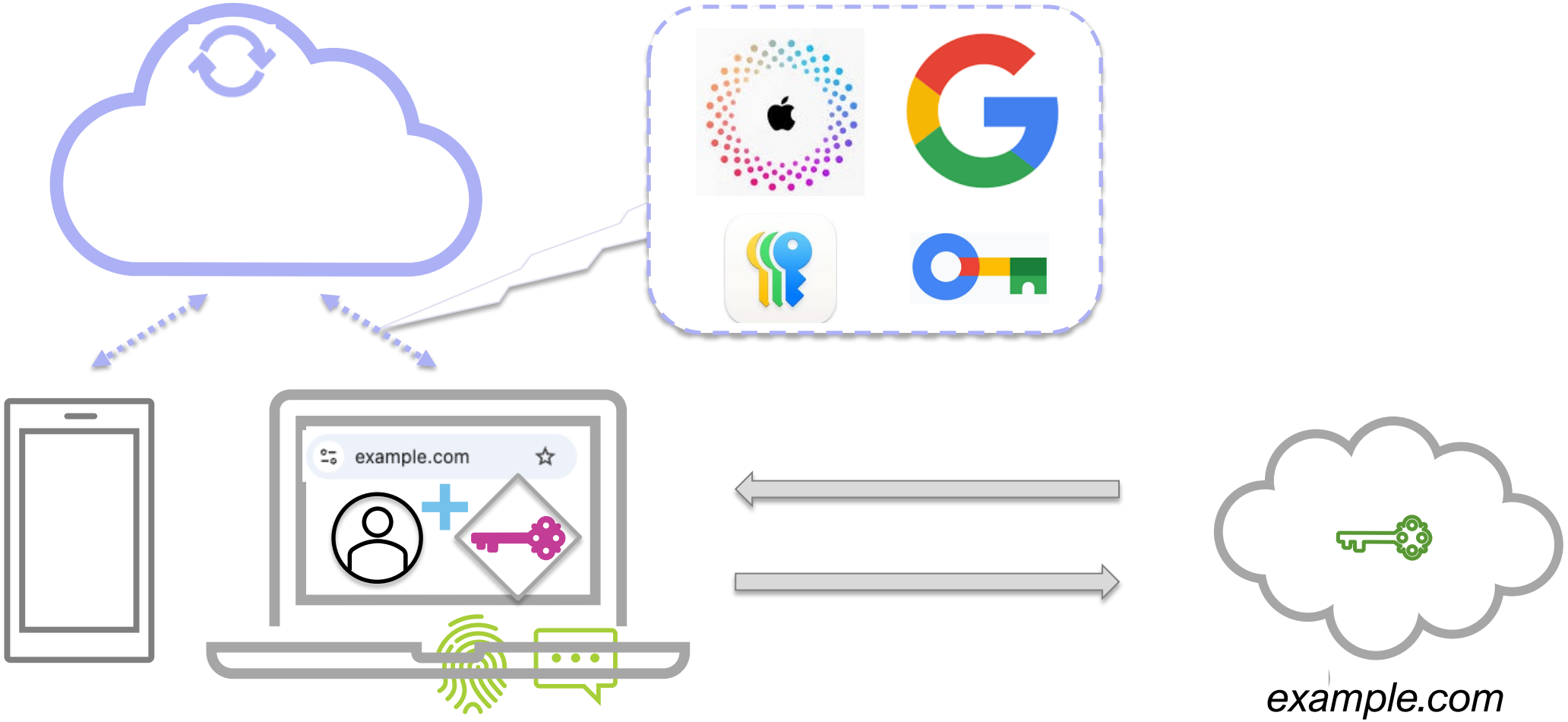


Passkey authentication is phishing-resistant.

Absolutely YES!

Synced passkeys provide a secure chain of trust.

Passkey chain of trust security considerations



Passkeys meet MFA requirements in a single step.

How are passkey factors used

App providers

Passkey providers

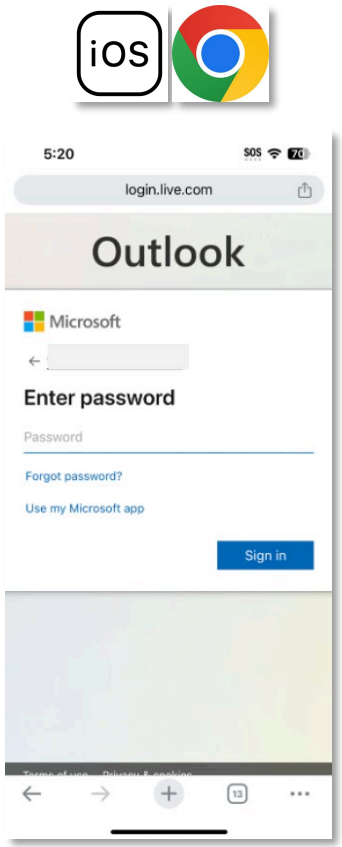
User devices

User interaction	Factor used	Factor counted by app	Passkey user experience
	1FA	1FA	
	2FA	2FA or 1FA	
	2FA	2FA or 1FA	

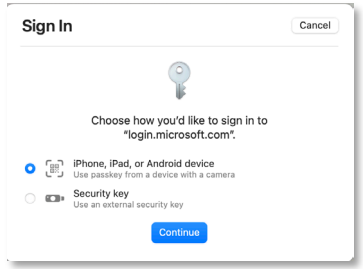
Users can use passkeys consistently across platforms.

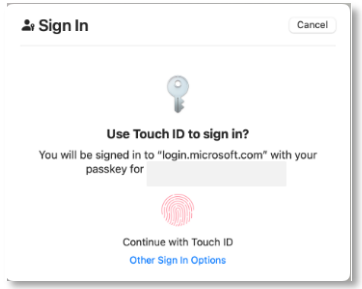
Inconsistent passkey login experience

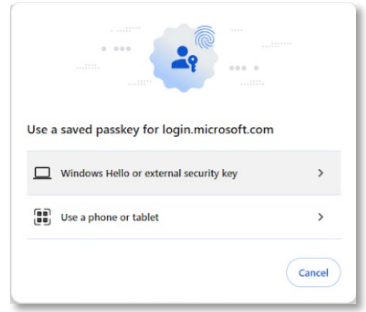
Microsoft
Face, fingerprint, PIN or security key
Your device will open a security window. Follow the instructions there to sign in.
Use your screen lock
Use your biometric to continue
Use passkey for login.microsoft.com
Use PIN
Terms of use
Privacy & cookies

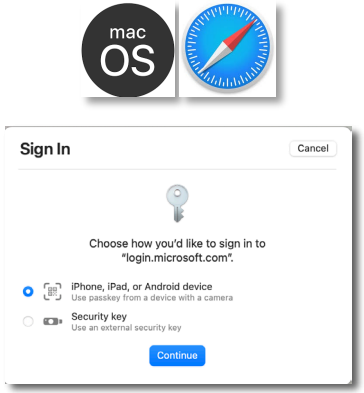


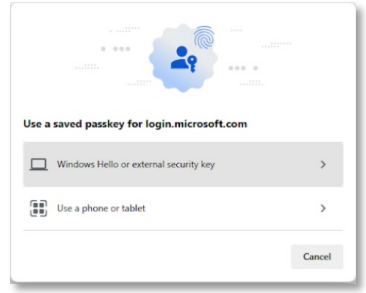
Microsoft
Face, fingerprint, PIN or security key
Your device will open a security window. Follow the instructions there to sign in.
Back
Sign In
Use Face ID to sign in?
You will be signed in to "microsoft.com" with your passkey for
Continue


Sign In
Cancel
Choose how you'd like to sign in to "login.microsoft.com".
iPhone, iPad, or Android device
Use passkey from a device with a camera
Security key
Use an external security key
Continue


Sign In
Cancel
Use Touch ID to sign in?
You will be signed in to "login.microsoft.com" with your passkey for
Continue with Touch ID
Other Sign In Options

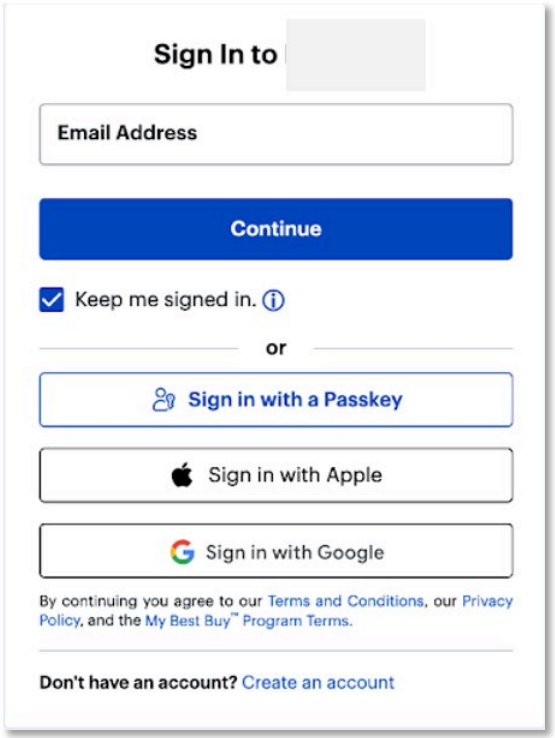


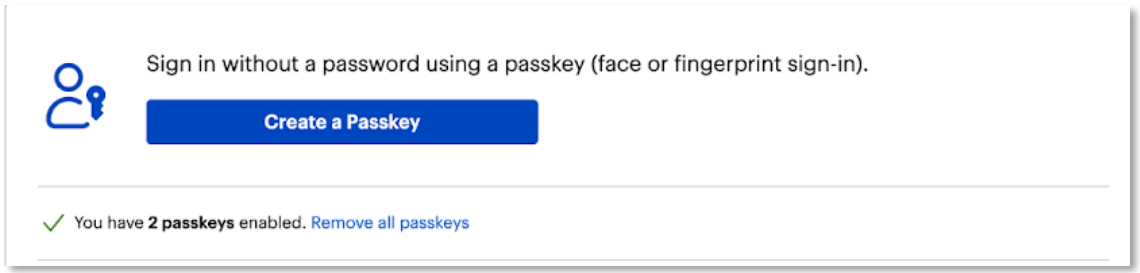

Sign In
Cancel
Choose how you'd like to sign in to "login.microsoft.com".
iPhone, iPad, or Android device
Use passkey from a device with a camera
Security key
Use an external security key
Continue

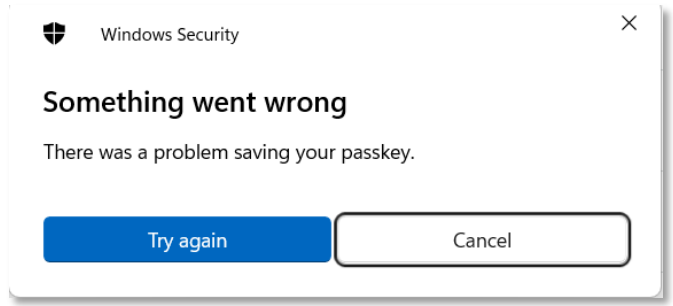


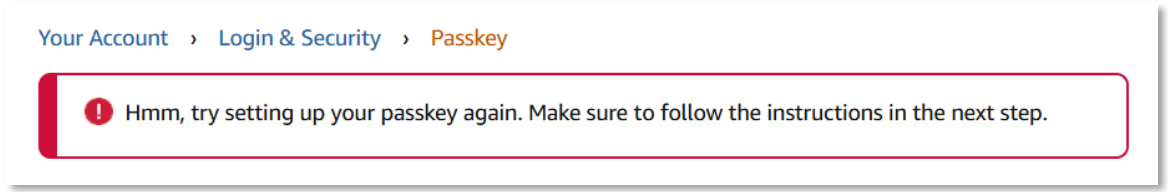
Applications implement passkeys in a secure and user-friendly way.

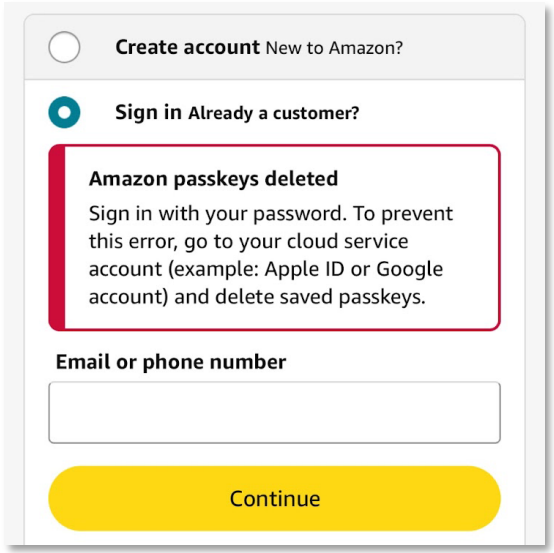
Challenges in the passkey lifecycle


Sign In to
Email Address
Continue
Keep me signed in.
or
Sign in with a Passkey
Sign in with Apple
Sign in with Google
By continuing you agree to our Terms and Conditions, our Privacy Policy, and the My Best Buy™ Program Terms.
Don't have an account? Create an account

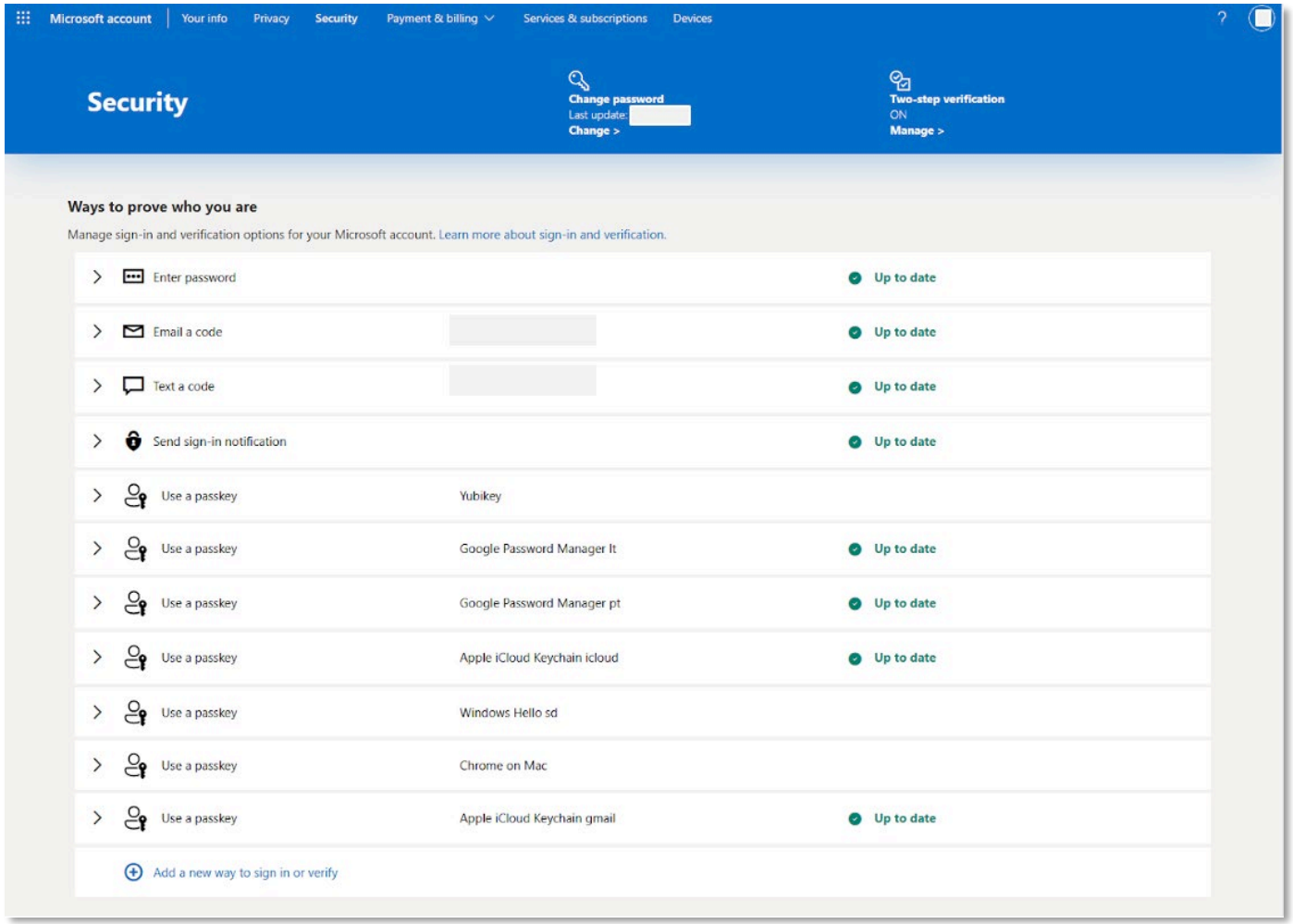

Sign in without a password using a passkey (face or fingerprint sign-in).
Create a Passkey
You have 2 passkeys enabled. Remove all passkeys




Your Account › Login & Security › Passkey
Hmm, try setting up your passkey again. Make sure to follow the instructions in the next step.

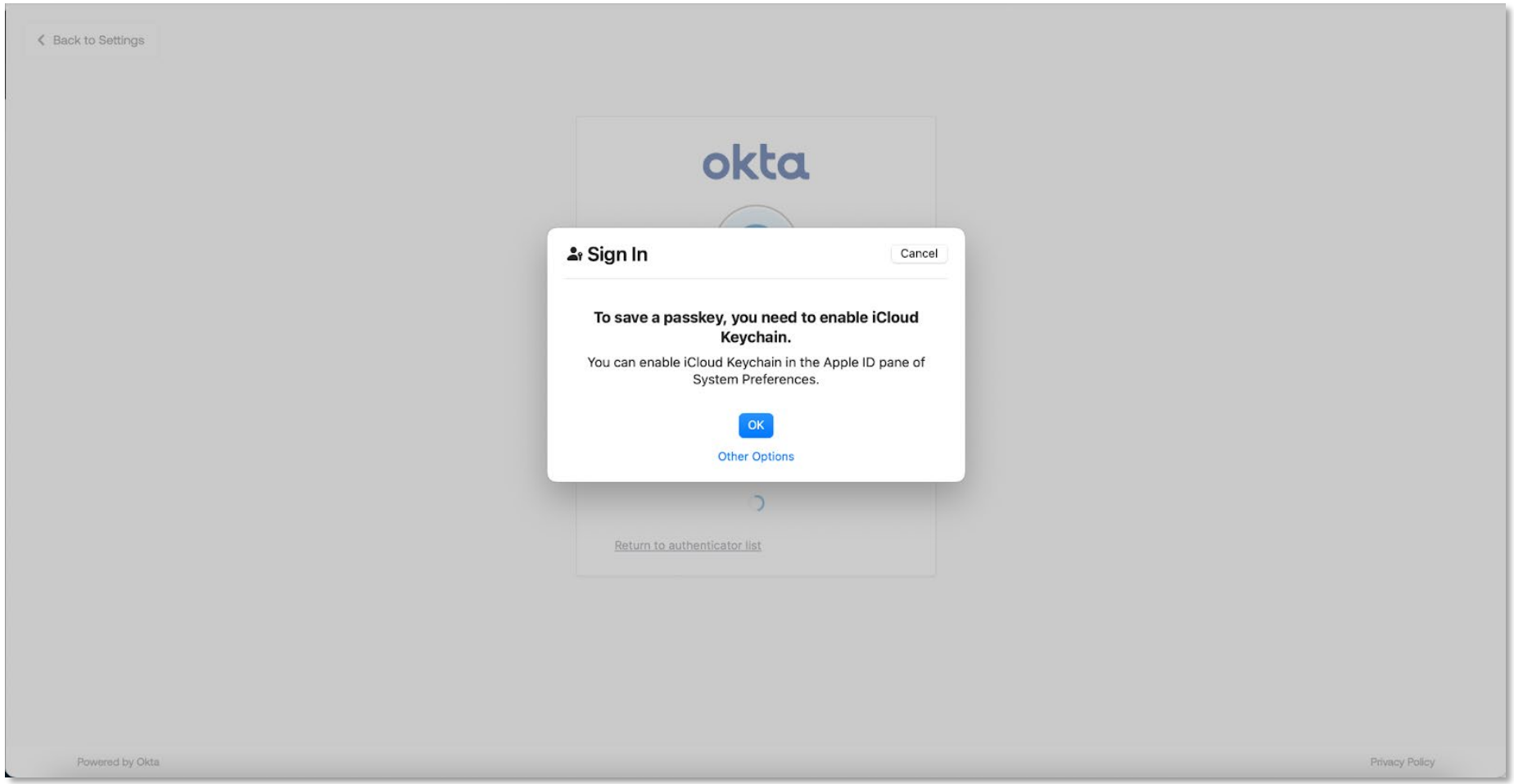

Create account New to Amazon?
Sign in Already a customer?
Amazon passkeys deleted
Sign in with your password. To prevent this error, go to your cloud service account (example: Apple ID or Google account) and delete saved passkeys.
Email or phone number
Continue

Credential sprawl reduces account security

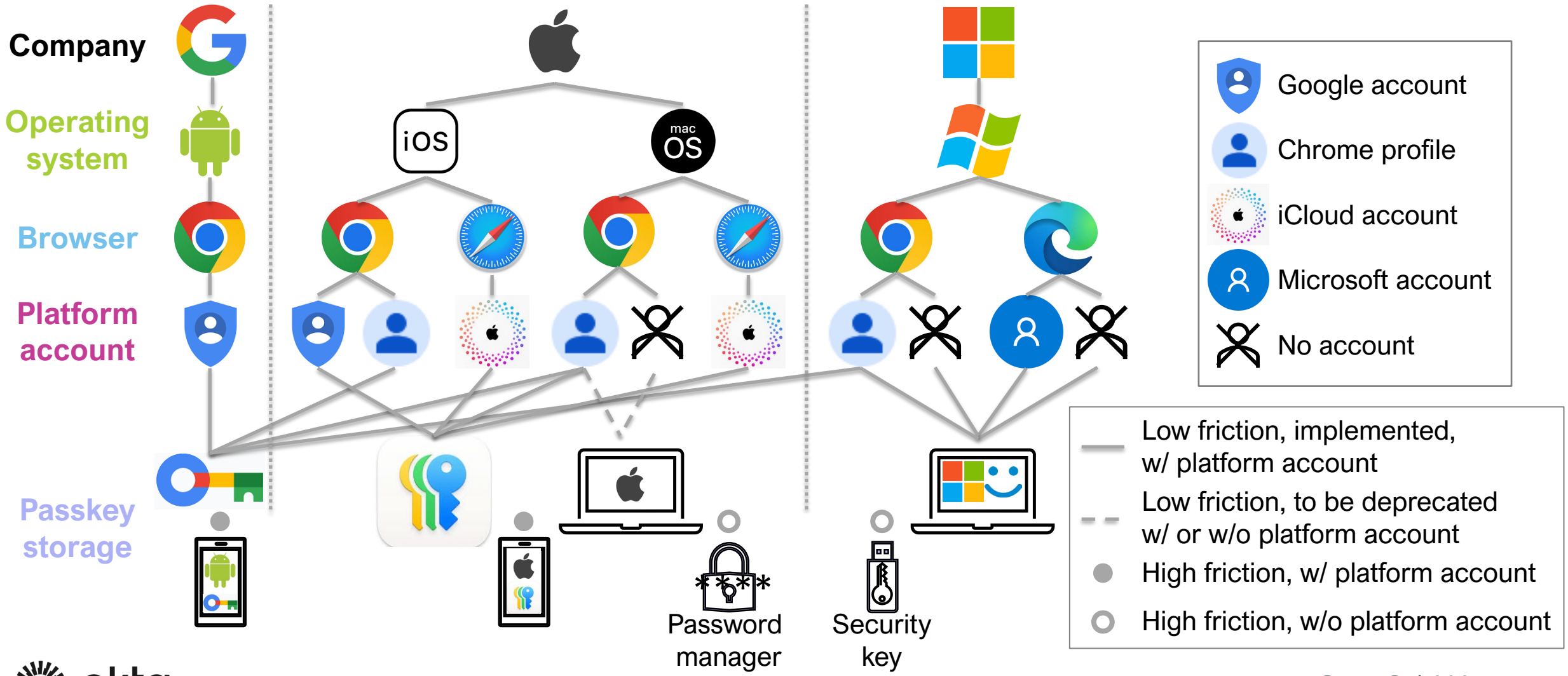


Users have the choice of whether to sync their passkeys.

Problem solving time



Passkey storage cheat sheet

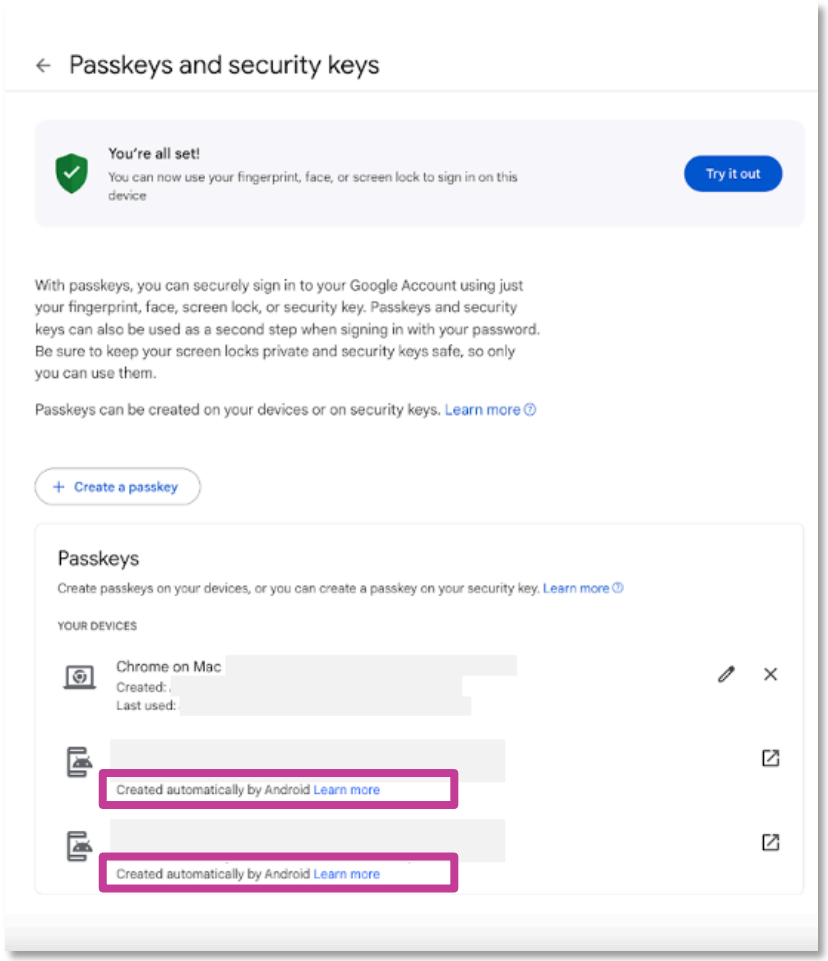


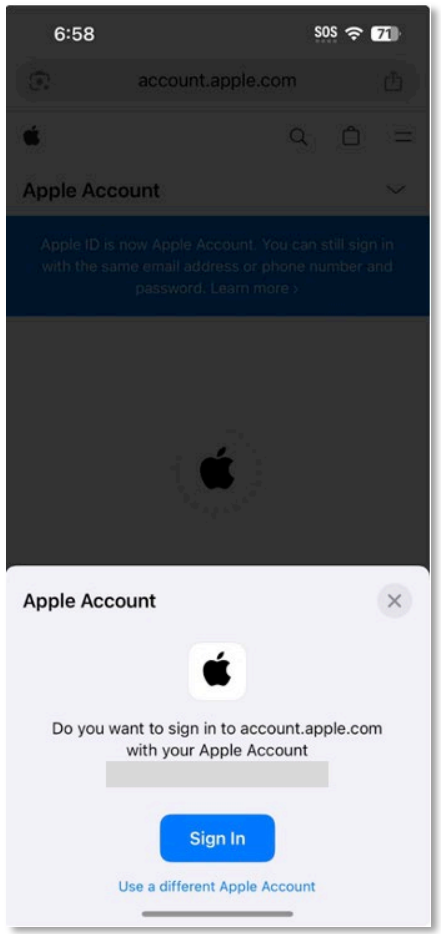
Will a superpower exist in the passkey era?

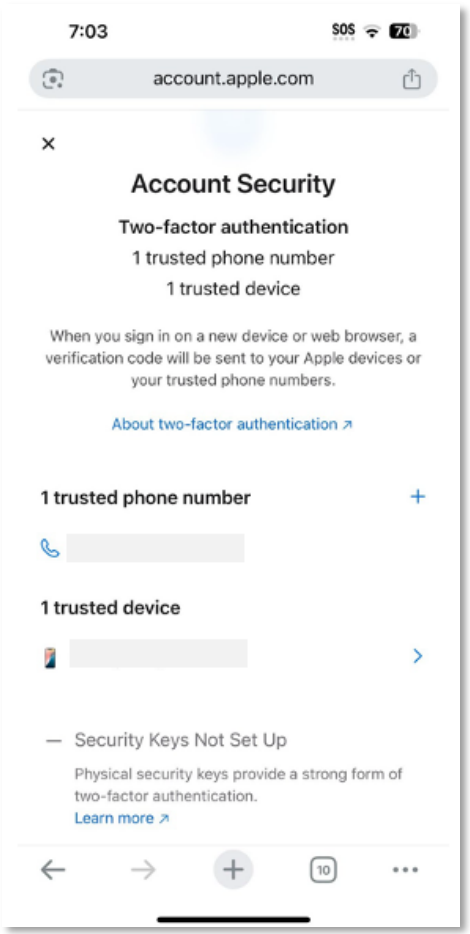
Dominant OS platform + Ubiquitous applications + Identity at scale

Users create their own passkeys.

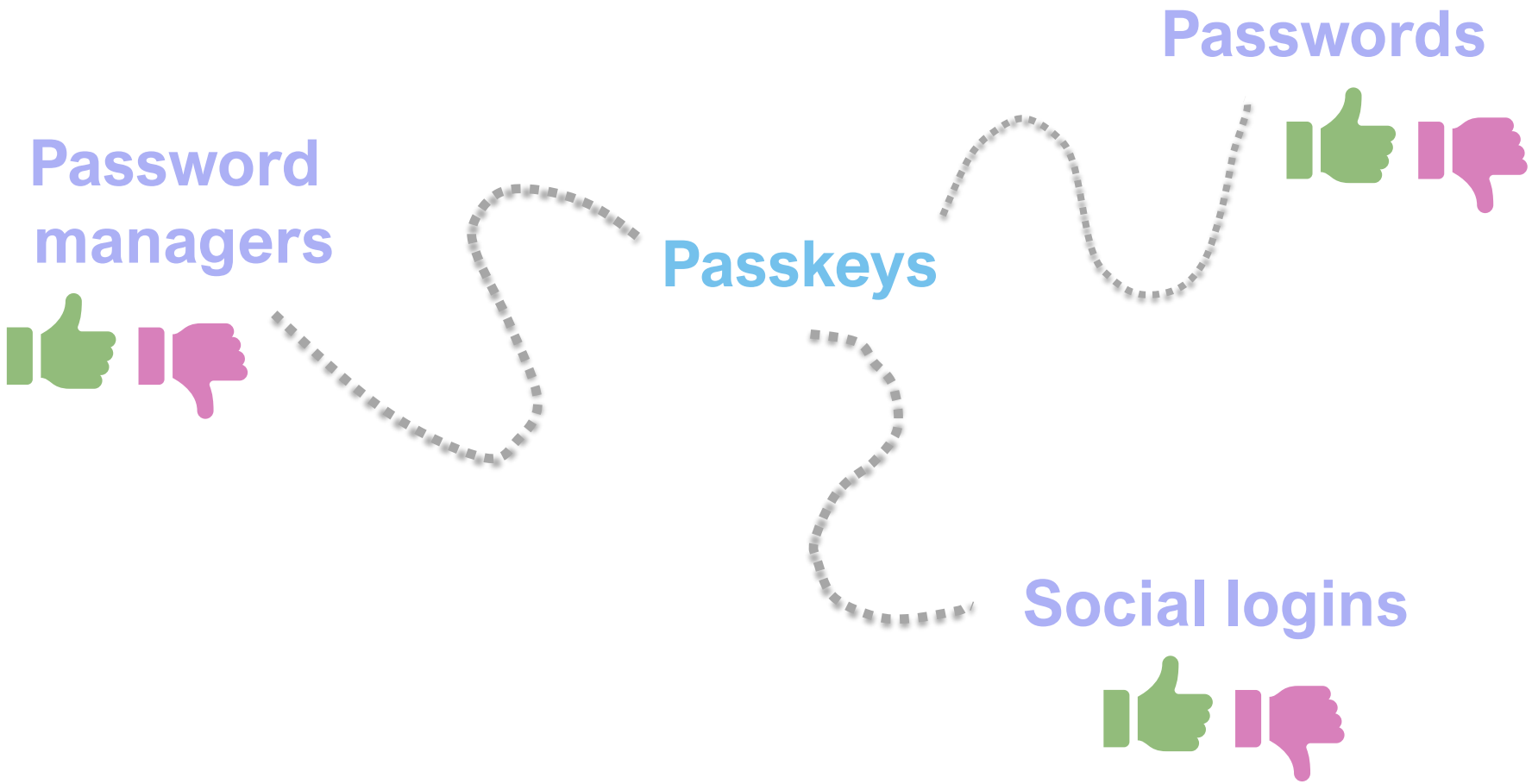
Auto-created passkeys are a double-edged sword

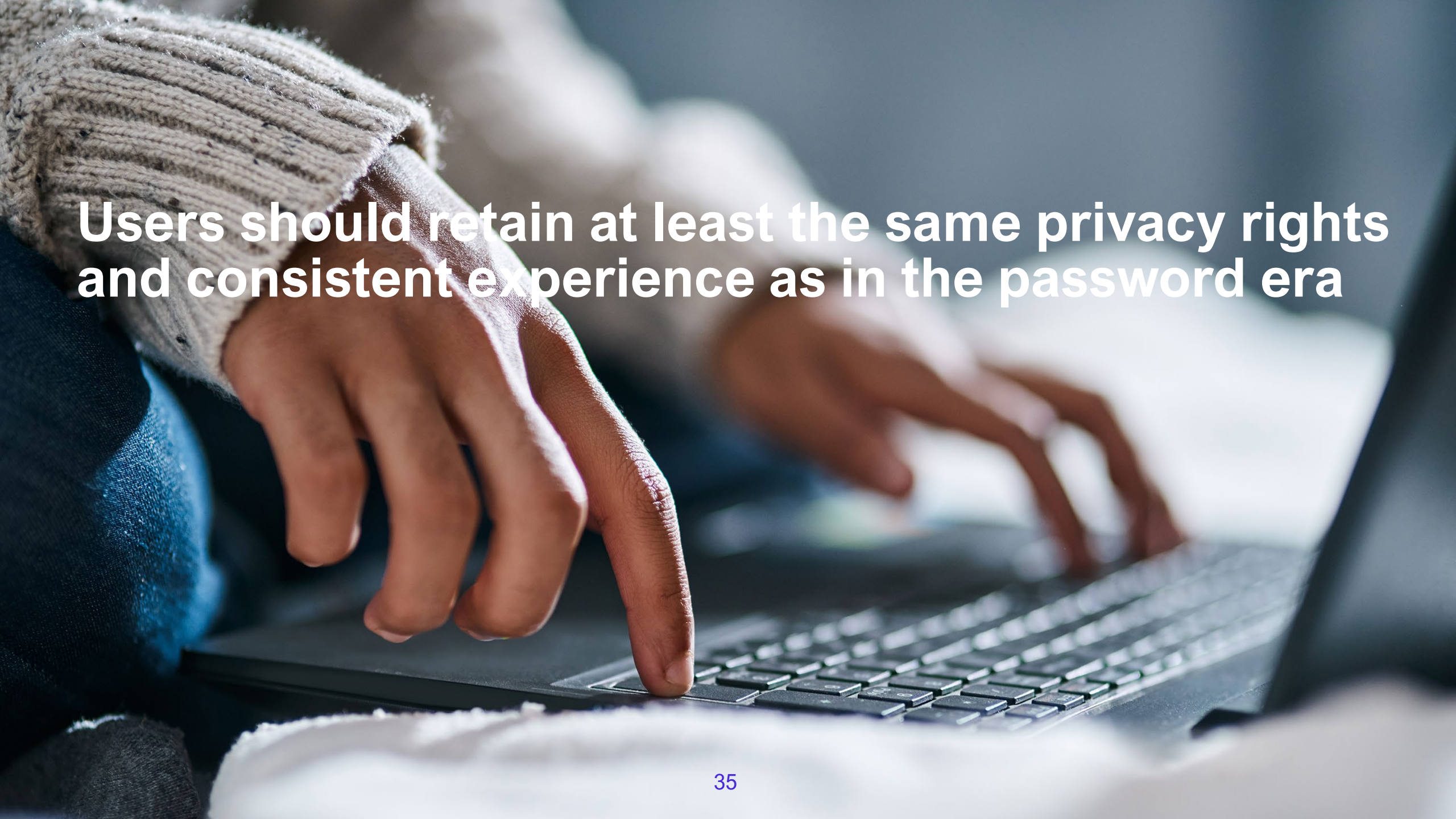

Passkeys and security keys
You're all set!
You can now use your fingerprint, face, or screen lock to sign in on this device
Try it out
With passkeys, you can securely sign in to your Google Account using just your fingerprint, face, screen lock, or security key. Passkeys and security keys can also be used as a second step when signing in with your password. Be sure to keep your screen locks private and security keys safe, so only you can use them.
Passkeys can be created on your devices or on security keys. Learn more
Create a passkey
Passkeys
Create passkeys on your devices, or you can create a passkey on your security key. Learn more
YOUR DEVICES
Chrome on Mac
Created:
Last used:
Created automatically by Android Learn more
Created automatically by Android Learn more


6:58
account.apple.com
Apple Account
Apple ID is now Apple Account. You can still sign in with the same email address or phone number and password. Learn more
Apple Account
Do you want to sign in to account.apple.com with your Apple Account
Sign In
Use a different Apple Account


7:03
account.apple.com
Account Security
Two-factor authentication
1 trusted phone number
1 trusted device
When you sign in on a new device or web browser, a verification code will be sent to your Apple devices or your trusted phone numbers.
About two-factor authentication
1 trusted phone number
1 trusted device
Security Keys Not Set Up
Physical security keys provide a strong form of two-factor authentication.
Learn more

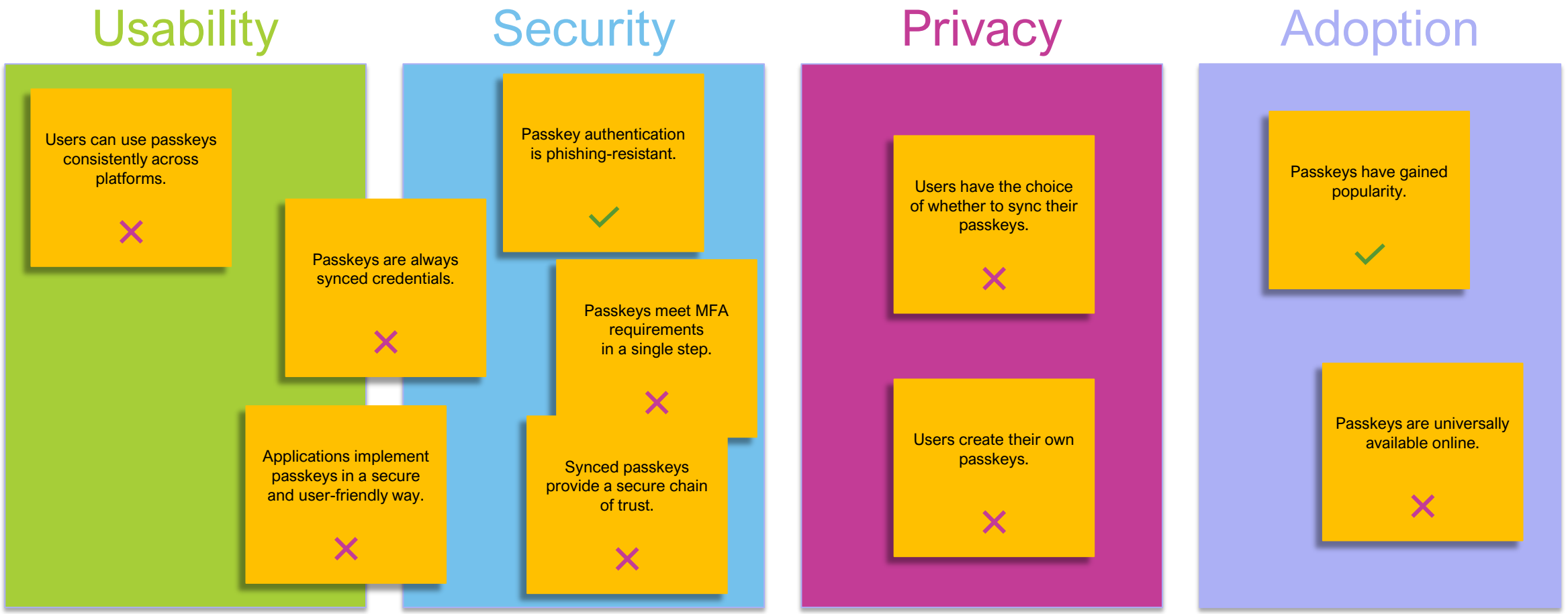
Passkeys vs. traditional logins



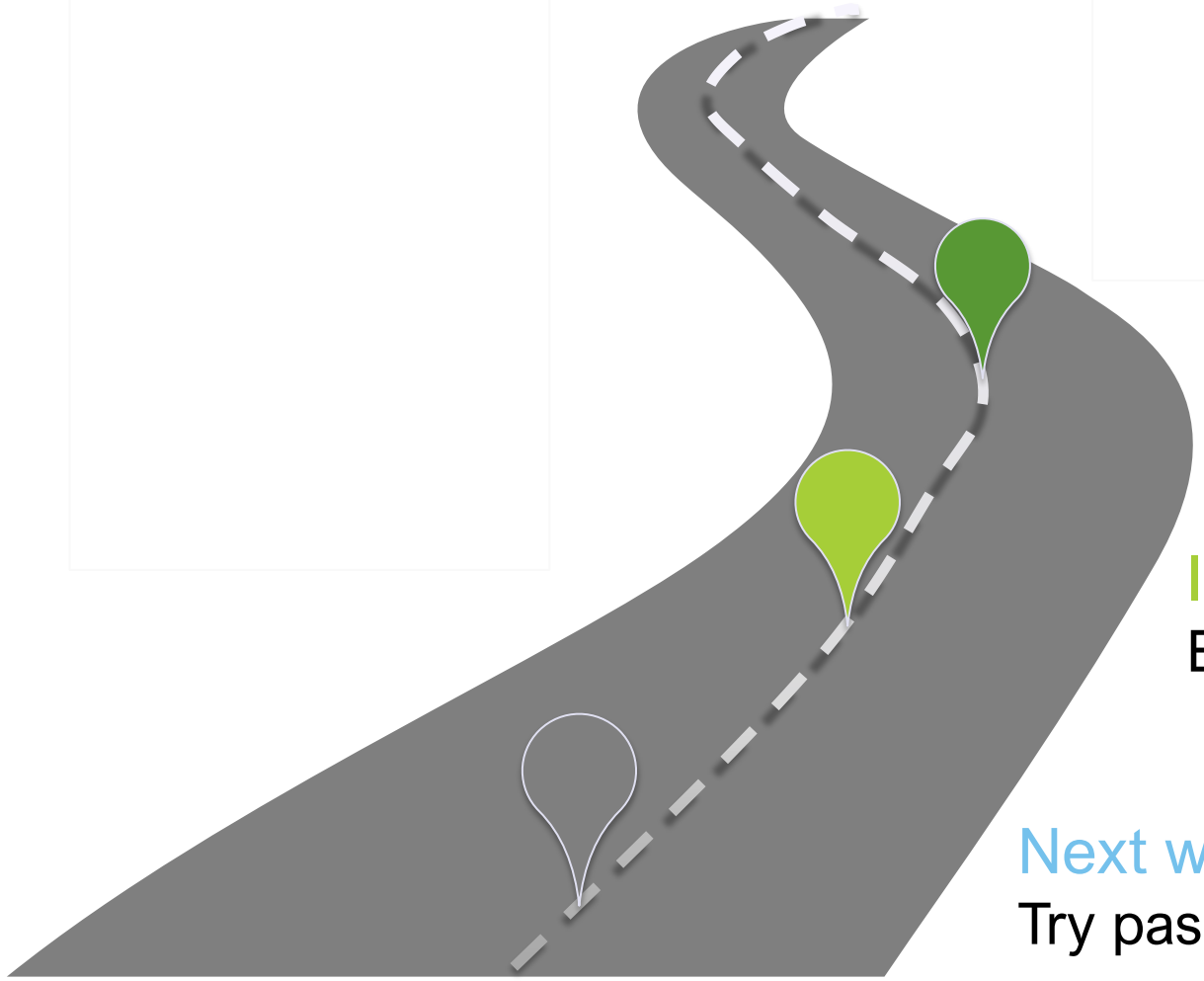

Users should retain at least the same privacy rights and consistent experience as in the password era

Snapshot of the current state of passkeys

Authenticator Framework


Usability
Users can use passkeys consistently across platforms.
Passkeys are always synced credentials.
Applications implement passkeys in a secure and user-friendly way.
Security
Passkey authentication is phishing-resistant.
Passkeys meet MFA requirements in a single step.
Synced passkeys provide a secure chain of trust.
Privacy
Users have the choice of whether to sync their passkeys.
Users create their own passkeys.
Adoption
Passkeys have gained popularity.
Passkeys are universally available online.

Apply what you have learned today



In six months

Prioritize users, speak up, and foster collaboration

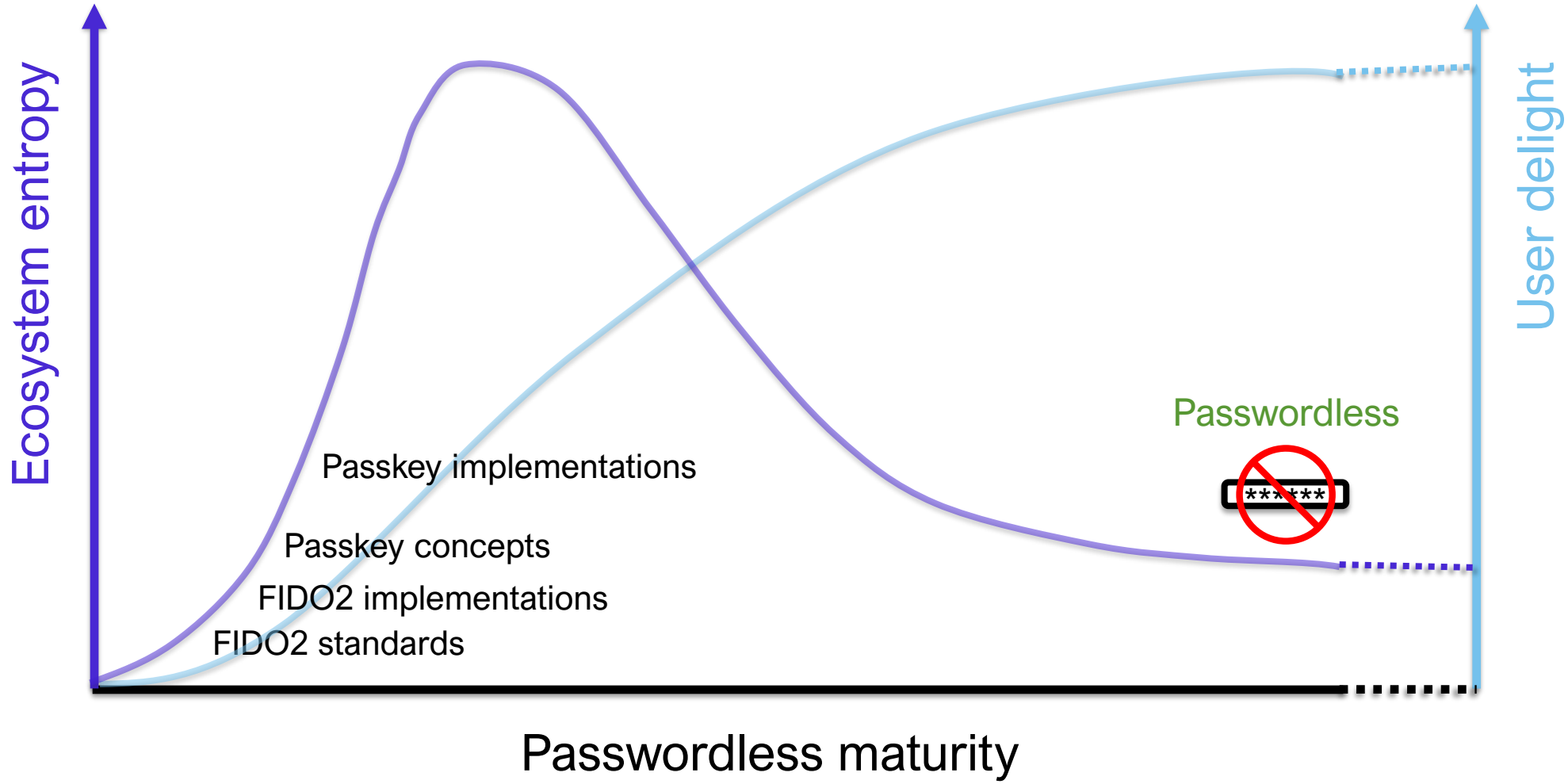
In three months

Evaluate passkey implementations

Next week

Try passkeys

Drive to the passwordless future



RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You